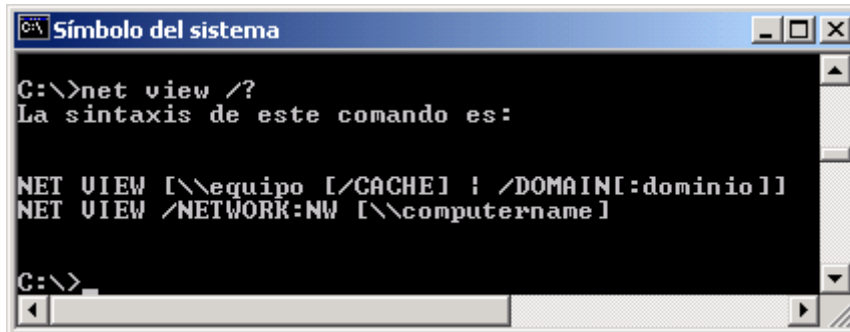


Práctica: 32.Herramientas del Sistema Operativo para obtener información

Net view listará los dominios disponibles en la red, es como usar el entorno de red y explorar.

Sintaxis:



```
C:\>net view /?
La sintaxis de este comando es:

NET VIEW [\\equipo [/CACHE] ; /DOMAIN[:dominio]]
NET VIEW /NETWORK:NW [\\computername]

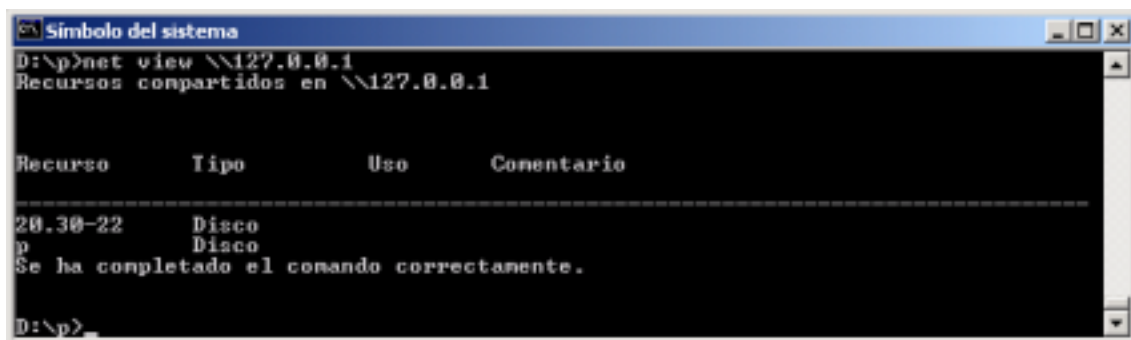
C:\>
```

Ejemplos:

C:\>net view /domain (mostrará todos los dominios disponibles desde el adaptador de red)

C:\>net view /domain:cursos (mostrará todas las máquinas que pertenezcan al dominio cursos)

Net view también puede mostrar la lista de recursos compartidos,



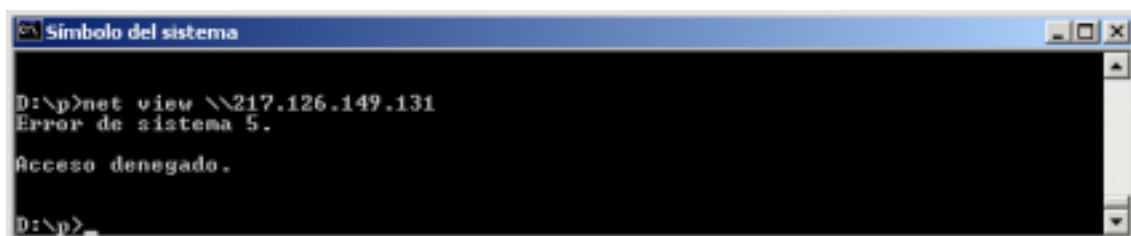
```
D:\p>net view \\127.0.0.1
Recursos compartidos en \\127.0.0.1

Recurso      Tipo      Uso      Comentario
-----
20.30-22     Disco
p            Disco
Se ha completado el comando correctamente.

D:\p>
```

Seguro, estas pensando.... ¿Y si hago Net view hacia una máquina remota?

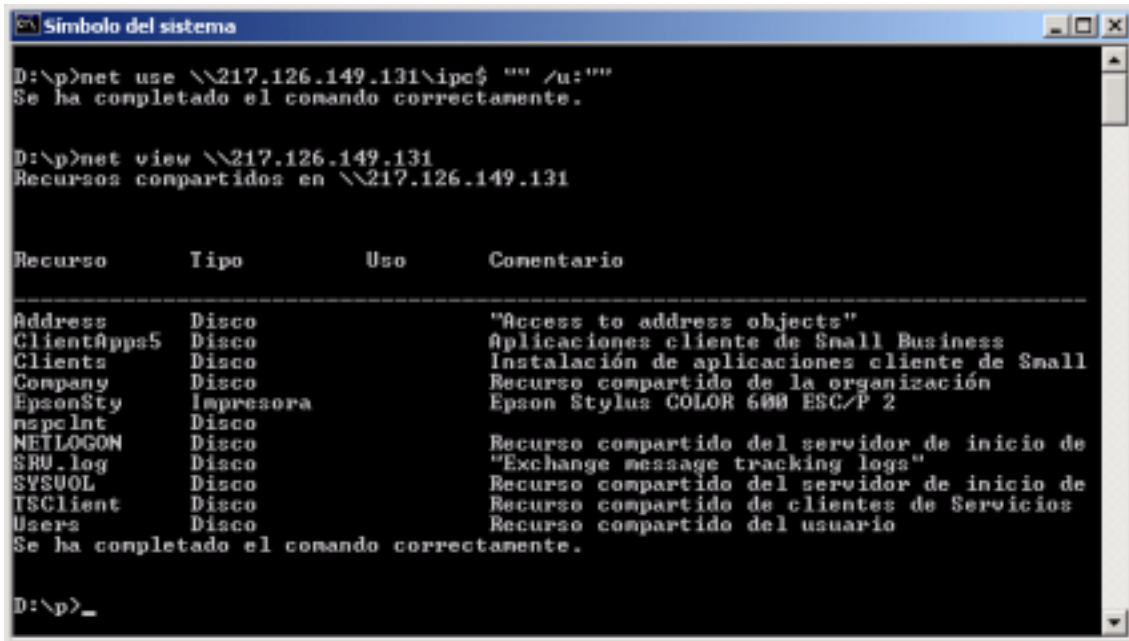
Prueba:



```
D:\p>net view \\217.126.149.131
Error de sistema 5.
Acceso denegado.

D:\p>
```

Como verás tienes negado el acceso, pero no está todo perdido, primero establecemos una sesión nula con el objetivo, y luego volvemos a probar netview:



```
Símbolo del sistema
D:\p>net use \\217.126.149.131\ipc$ "" /u:""
Se ha completado el comando correctamente.

D:\p>net view \\217.126.149.131
Recursos compartidos en \\217.126.149.131

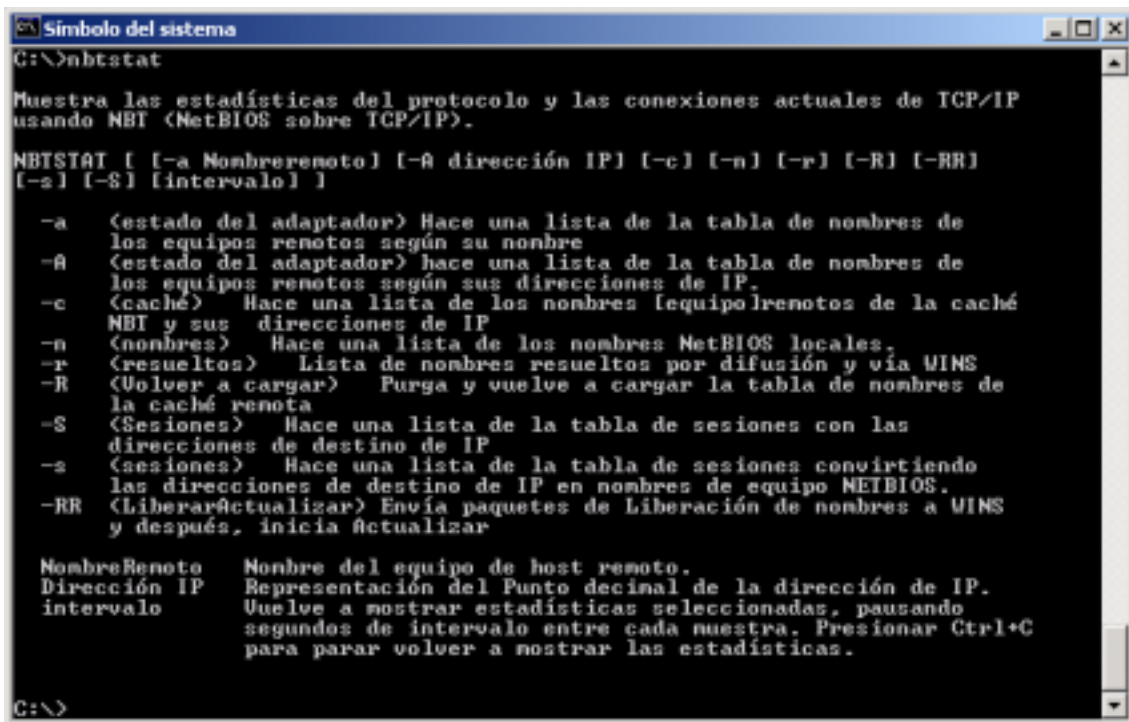
Recurso      Tipo      Uso      Comentario
-----
Address      Disco    "Access to address objects"
ClientApps5  Disco    Aplicaciones cliente de Small Business
Clients      Disco    Instalación de aplicaciones cliente de Small
Company      Disco    Recurso compartido de la organización
EpsonSty     Impresora
             Disco    Epson Stylus COLOR 600 ESC/P 2
npclnt      Disco
NETLOGON     Disco    Recurso compartido del servidor de inicio de
SRU.log      Disco    "Exchange message tracking logs"
SYSVOL       Disco    Recurso compartido del servidor de inicio de
TSCClient    Disco    Recurso compartido de clientes de Servicios
Users        Disco    Recurso compartido del usuario
Se ha completado el comando correctamente.

D:\p>_
```

Ahora sí. Tenemos los recursos compartidos del objetivo.

Otra buena herramienta integrada en el Sistema Operativo es *nbtstat*

Sintaxis:



```
Símbolo del sistema
C:\>nbtstat

Muestra las estadísticas del protocolo y las conexiones actuales de TCP/IP
usando NBT (NetBIOS sobre TCP/IP).

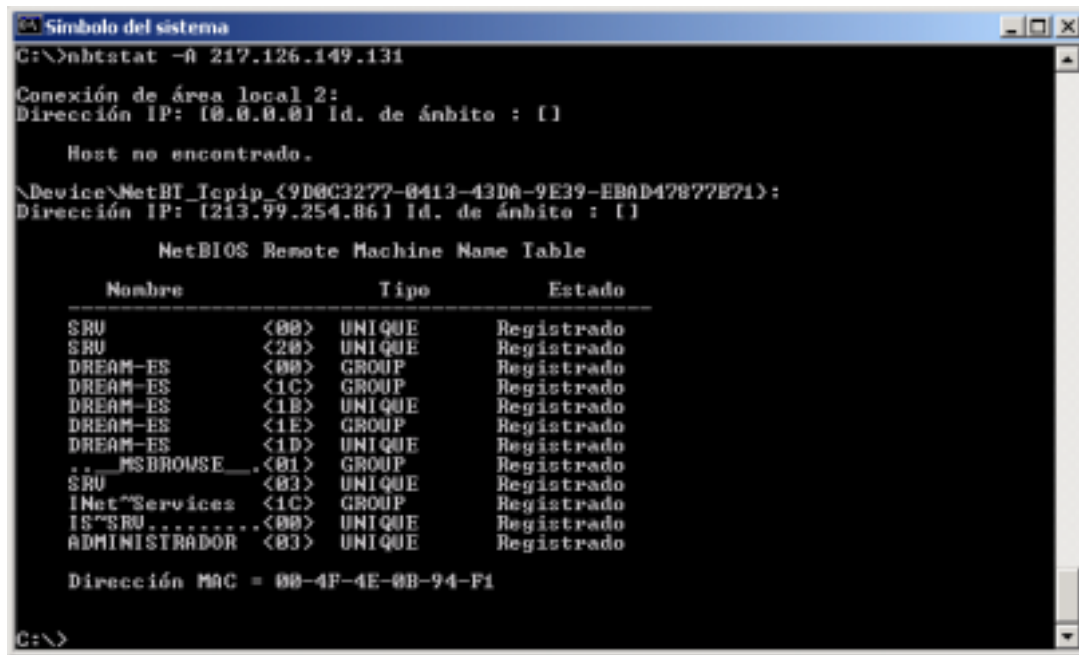
NBTSTAT [ [-a NombreRemoto] [-A dirección IP] [-c] [-n] [-r] [-R] [-RR]
[-s] [-S] [intervalo] ]

-a <estado del adaptador> Hace una lista de la tabla de nombres de
los equipos remotos según su nombre
-A <estado del adaptador> hace una lista de la tabla de nombres de
los equipos remotos según sus direcciones de IP.
-c <caché> Hace una lista de los nombres [equipos]remotos de la caché
NBT y sus direcciones de IP
-n <nombres> Hace una lista de los nombres NetBIOS locales.
-r <resueltos> Lista de nombres resueltos por difusión y vía WINS
-R <Volver a cargar> Purga y vuelve a cargar la tabla de nombres de
la caché remota
-S <Sesiones> Hace una lista de la tabla de sesiones con las
direcciones de destino de IP
-s <sesiones> Hace una lista de la tabla de sesiones convirtiendo
las direcciones de destino de IP en nombres de equipo NETBIOS.
-RR <LiberarActualizar> Envía paquetes de Liberación de nombres a WINS
y después, inicia Actualizar

NombreRemoto Nombre del equipo de host remoto.
Dirección IP Representación del Punto decimal de la dirección de IP.
intervalo Vuelve a mostrar estadísticas seleccionadas, pausando
segundos de intervalo entre cada muestra. Presionar Ctrl+C
para parar volver a mostrar las estadísticas.

C:\>
```

Ejemplos



Nbtstat extrae una tabla de nombres *netbios* de una máquina, y entre otras cosas nos informa del dominio a que pertenece, de cualquier usuario que haya iniciado una sesión y de su dirección MAC.

Los sufijos Netbios <00>, <20>, etc significan lo siguiente:

Sufijo	Servicio
<00>	Estación de trabajo
<20>	Servidor
<1C>	Controlador de Dominio y/o IIS
<1B>	Explorador Principal de Dominio
<1E>	Elecciones del servicio del explorador
<1D>	Explorador Principal
<01>	Mensajería. Para mensajes enviados a esta máquina
<03>	Mensajería

Existen muchos más sufijos, por ejemplo

Sufijo	Servicio
<06>	Servidor RAS
<21>	Cliente RAS
<30>	Servidor para compartir Módems
<1F>	NetDDE
<22>	Intercambio de MS Exchange
<23>	Almacén de MS Exchange
<24>	Directorio de MS Exchange

Todavía hay más, pero con estos son suficientes, debes prestar atención a la columna nombre Netbios, en el volcado anterior aparecen dos sufijos Netbios <1C> uno para el nombre DREAM-ES y otro para el nombre Inet Services.

Como <1C> significa servidor, podemos entender que se trata de un servidor de dominio y servidor Web (IIS) integrados en la misma máquina.

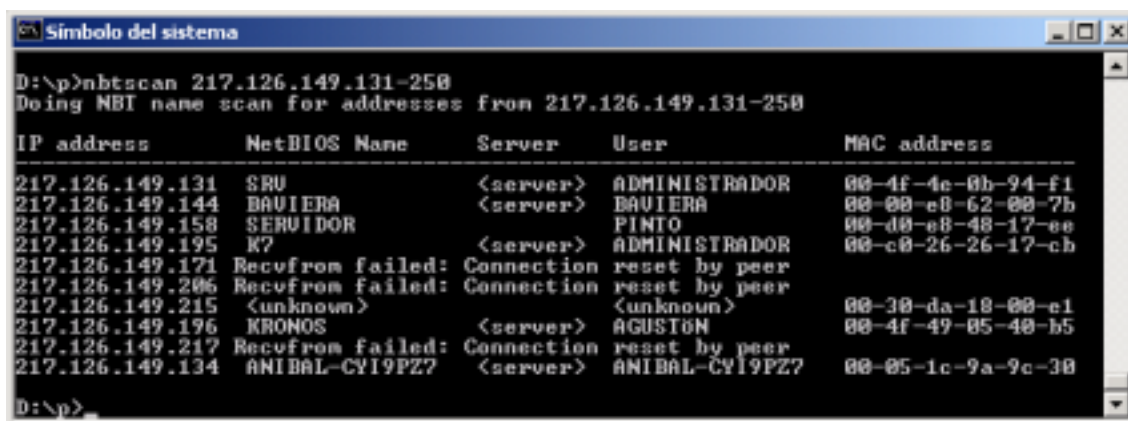
También es interesante la columna Tipo, que puede ser:

Unique: El nombre tiene una única dirección IP asignada

Group: Un único nombre pero pueden tener asignadas muchas direcciones IP

Múltiple: El nombre es único, pero puede existir en múltiples interfaces del mismo equipo.

Una herramienta de “terceros” que hace prácticamente lo mismo pero con una salida más comprensible es nbtscan, que además puede escanear una red completa y no un solo equipo.



```
D:\p>nbtscan 217.126.149.131-250
Doing NBT name scan for addresses from 217.126.149.131-250

IP address      NetBIOS Name    Server      User          MAC address
-----
217.126.149.131 SRU              <server>    ADMINISTRADOR 00-4f-4c-0b-94-f1
217.126.149.144 BAUIERA         <server>    BAUIERA        00-00-e8-62-00-7b
217.126.149.158 SERVIDOR        <server>    PINTO          00-d0-e8-48-17-ee
217.126.149.195 K?              <server>    ADMINISTRADOR 00-c0-26-26-17-ch
217.126.149.171 Recvfrom failed: Connection reset by peer
217.126.149.206 Recvfrom failed: Connection reset by peer
217.126.149.215 <unknown>       <unknown>    <unknown>      00-30-da-18-00-e1
217.126.149.196 KRONOS          <server>    AGUSTÓN        00-4f-49-05-40-b5
217.126.149.217 Recvfrom failed: Connection reset by peer
217.126.149.134 ANIBAL-CY19PZ? <server>    ANIBAL-CY19PZ? 00-05-1c-9a-9c-38

D:\p>
```

Otra más, nltest

Permite identificar a los controladores de dominio, para ello escribe:

```
C:\>nltest /dclist:ursos
```

Y se mostrarán los controladores de dominio para el dominio cursos.

Otras herramientas que no debes olvidar y probar son:

NetInfo, Netview.exe, lanhunter, getmac, DumpSec e IPtools

Y mas...

De todas ellas son bastante interesantes:

LanHunter: que busca recursos compartidos en una Red

DumpSec: Además de enumerar Recursos compartidos, también usuarios, Registro, Grupos, etc.

IpTools: Es “un todo en uno” Escanea y descubre recursos NetBios, Telnet, Escanea puertos, Transferencias de Zonas, Whois, nos muestra las conexiones activas, etc. Es una muy buena utilidad. DEBES PROBARLA